Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method for encrypted data storage in a storage system, the method comprising:

converting blocks of data to produce corresponding converted blocks of data, wherein a converted block of data is encrypted with cryptographic criteria;

receiving and processing a read request during said converting in order to access read data from said storage system and in response thereto accessing said read data from at least one decrypted block of data, wherein said read data is decrypted from one converted block of said converted blocks of data using said cryptographic criteria to produce said at least one decrypted block of data.

2. (previously presented) The method of claim 1 wherein said converting comprises replacing each encrypted block of data by a corresponding converted block of data thereof.

3. (previously presented) The method of claim 1 wherein some of said encrypting and decrypting comprise executing computer program code on a data processing component.

4. (previously presented) The method of claim 2 further comprising accessing at least one of said cryptographic criteria over a communication network.

5. (previously presented) The method of claim 1 wherein some of said encrypting and decrypting are performed on logic circuitry configured to perform cryptographic operations.

6. (previously presented) The method of claim 1 wherein said read request is a file-level read request and said accessing said read data includes producing one or more block-level read requests based on said file-level read request.

7. (canceled)

8. (canceled)

9. (currently amended) In a storage system including a storage device, the storage system being coupled to a host device via a network, a method for storing encrypted data comprising:

converting a plurality of first data blocks of said storage system to produce a plurality of corresponding second data blocks, including encryption with cryptographic criteria to produce said plurality of second data blocks and replacing each first data block with a corresponding second data block thereof; and

accessing read data from said storage device in response to a read request from the host device, including reading a third data block and decrypting said third data block with the cryptographic criteria [[if]] wherein said third data block is one of said plurality of second data blocks, to return said decrypted third data block to said host device,

wherein said step of accessing read data is performed during said step of converting.

10. (previously presented) The method of claim 9 further comprising storing a fourth data block to said storage device in response to a write request from the host device, said fourth data block comprising data to be written, said step of storing including encrypting said fourth data block with the cryptographic criteria if said fourth data block is to be written to one of said second data blocks, wherein said step of storing is performed during said step of converting.

11. (original) The method of claim 9 wherein said first data blocks are not encrypted.

12. (previously presented) The method of claim 9 wherein said first data blocks are encrypted with first cryptographic criteria different from said cryptographic criteria, and wherein converting first data blocks includes decrypting said first data blocks with the first cryptographic criteria prior to encryption with said cryptographic criteria.

13. (previously presented) The method of claim 12 wherein said step of accessing read data from said storage device in response to a read request from the host device includes reading a third data block and decrypting said third data block with the first cryptographic criteria if said third data block is one of said first data blocks.

14. (previously presented) The method of claim 13 further comprising storing a fourth data block to said storage device in response to a write request from the host device, said fourth data block comprising data to be written, said step of storing comprising:

encrypting said fourth data block with said cryptographic criteria if said fourth data block is to be written to one of said second data blocks,

wherein said step of storing is performed during said step of converting.

15. (currently amended) A storage system comprising:

a storage component; and

a cryptographic component in data communication with said storage component and operable to convert a plurality of unconverted blocks of data stored thereon to produce a plurality of corresponding converted blocks of data, each converted block of data replacing a corresponding unconverted block of data thereof on said storage component and in the same location as said corresponding unconverted block of data thereof,

wherein said cryptographic component is further operable to receive and process read and write requests for data stored on said storage component, while said plurality of unconverted blocks of data are converted to said plurality of converted blocks of data,

wherein said cryptographic component is further operable to process a read request by accessing read blocks associated with said read request from said storage

component, wherein if a read block is one of said unconverted blocks of data, then performing a first cryptographic process on said read block to produce an unencrypted read block, wherein if said read block is one of said converted blocks of data, then performing a second cryptographic process on said read block to produce an unencrypted read block,

wherein said cryptographic component is further operable to process a write request by writing one or more write blocks associated with said write request from said storage component, wherein if a write block is to be written to a block location that contains an unconverted block, then performing said first cryptographic process on said write block prior to writing said write block, wherein if a write block is to be written to a block location that contains a converted block, then performing said second cryptographic process on said write block prior to writing said write block.

16. (original) The storage apparatus of claim 15 further comprising a file system component configured to receive file-level read and write requests from one or more host devices, to produce said read and write requests based on said file-level read and write requests, and to communicate said read and write requests to said cryptographic component.

17. (original) The storage apparatus of claim 15 wherein said storage component comprises an I/O interface and said cryptographic component comprises a first I/O interface and a second I/O interface, wherein said first I/O interface is configured for communication with a host device, wherein said second I/O interface is in data communication with said I/O interface of said storage component.

18. (original) The storage apparatus of claim 15 wherein said cryptographic component comprises one or more encryption engines.

19. (original) The storage apparatus of claim 15 wherein said cryptographic component is further operable to obtain criteria which specify said second cryptographic process prior to converting unconverted blocks of data to converted blocks of data.

20. (original) The storage process of claim 15 wherein said first cryptographic process is a NULL process.

21. (previously presented) A method for storing and accessing data on a storage system comprising:

receiving from a host device file-level I/O requests;

converting blocks of data stored in said storage system, including for each block of data:

performing a first decryption of said block of data to produce an unencrypted block of data, said block of data being encrypted by a first encryption;

performing a second encryption of said unencrypted block of data to produce an encrypted block of data; and

overwriting said block of data with said encrypted block of data encrypted by said second encryption;

during said converting, receiving and servicing a file-level read request; and

during said converting, receiving and servicing a file-level write request,

wherein servicing said file-level read request comprises:

producing one or more block-level read operations; and

decrypting a corresponding block of said block-level read operation with either said first or second decryption depending on how said block was encrypted during said converting,

wherein servicing said file-level write request comprises:

producing one or more block-level write operations;

encrypting a corresponding block of data of said block-level write operation with said first encryption, if said block-level write operation is targeted to a block location in said storage system containing data that was encrypted with said first encryption during said converting; and

encrypting said corresponding block of data of said block-level write operation with said second encryption, if said block-level write operation is targeted to a block location in said storage system containing data that was encrypted with said second encryption during said converting.

22. (previously presented) The method of claim 21 wherein some of said encrypting and decrypting comprise executing computer program code on a data processing component.

23. (original) The method of claim 22 further comprising accessing at least one of said encryption and decryption criteria over a communication network.

24. (previously presented) The method of claim 21 wherein some of said encrypting and decrypting are performed on logic circuitry configured to perform cryptographic operations.

25. (previously presented) The method of claim 21 wherein said blocks of data are converted in sequential order as said blocks of data are stored in said storage system.

26. (canceled)

27. (previously presented) The method of claim 1 further comprising receiving a write request during said converting in order to store write data to said storage system and in response thereto writing at least a first block of data to said storage system, said first block of data comprising data to be written, wherein if said first block of data is targeted to a converted block of data, then encrypting at least some of said converted block of data using said cryptographic criteria to produce said first block of data.

28. (previously presented) The method of claim 27 wherein said write request is a file-level write request and said writing at least a first block of data includes producing one or more block-level write requests based on said file-level write request.

29. (previously presented) The method of claim 28 wherein said file-level read request and said file-level write request are received from a host device.

30. (previously presented) In a storage system including a storage device, the storage system being coupled to a host device via a network, a method for storing encrypted data comprising:

converting a plurality of first data blocks of said storage system to produce a plurality of corresponding second data blocks, including encryption with cryptographic criteria to produce said second data blocks and replacing each first data block with a corresponding second data block thereof;

receiving a read request from the host device; and

returning a third data block, said third data block being decrypted from one of said plurality of second data blocks with said cryptographic criteria;

wherein said receiving a read request and said returning third data block are performed during said converting the plurality of first data blocks.

31. (previously presented) The method of claim 30, wherein replacing each first data block with a corresponding second data block thereof comprises overwriting each first data block with a corresponding second data block thereof.

32. (previously presented) The method of claim 30, further comprising:

receiving a write request with a fourth data block in a prescribed data form from the host device,

wherein the returned third data block to the host device is in the prescribed data form.